Compatible Systems Setup Guides: Network Address Translation Configuration Guide

Document ID: 17621

Contents − Network Address Translation Configuration Guide

EXTERNAL NAT PORT

INTERNAL NAT PORT

[IP < Secton ID >] configure commands and example keywords for **Example Three**

EXTER NAL NAT PORT

INTERNAL NAT PORT

NAT PASSTHRU RANGE

FINAL NOTES

IMPORTANT DISCLAIMERS

1. Not all Compatible Systems devices have Network Address Translation ability. Due to memory limitations and software code size, the following routers **do not** have NAT software:
    - ♦ MicroRouter 900i
    - ♦ MicroRouter 1000R
    - ♦ RISC Router 3000E
    - ♦ RISC Router 3400R
    - ♦ RISC Router 3800R
2. NAT functionality is available on Compatible Systems device IP interfaces with one important exception. A WAN interface can be used as the NAT external port **only** if its IP address is assigned in the device's configuration. NAT cannot function on a WAN interface which has its IP address assigned by a dial−up, PPP negotiation.
3. Compatible Systems NAT implementation supports Real Audio and CUSeeMe.
4. The NAT software in Compatible Systems devices does not yet support several IP Applications. Some of the more popular IP applications not yet supported are:
    - ♦ IRC (Internet Relay Chat)
    - ♦ X Windows
    - ♦ IPSec

EXPLANATION OF NAT FUNCTIONALITY

Reasons for Network Address Translation

IP Address Availability

The Internet is still growing at an almost exponential rate, with a finite number of Internet Protocol (IP) addresses available. Several solutions to this future shortage of IP addresses have been proposed and are currently being developed. One of the solutions currently being used is Network Address Translation (NAT).

NAT can ease the IP address shortage by creating "local" or "private" networks (also referred to as NAT Networks in this document) which are connected to the "official" Internet/External Network using only a single "global" IP address. This "global" IP address would have originally been assigned by the Internet Network Information Center (InterNIC), probably through an Internet Service Provider (ISP) or System Administrator.

For example, a private group can create a local network of ten workstations with an IP addressing system which is totally independent of the Internet, and connect their network to the Internet with one "global" Internet IP address. In this case, the group would only need a

single IP address supplied by an ISP or the company System Administrator, rather than an IP address for each workstation −− a savings of nine valuable IP addresses.

Local Network Security

Another useful feature of NAT is its ability to act as a "firewall." The workstations on the NAT Network may freely establish connections with the External Network/Internet. The opposite case is possible, but is controlled by NAT. NAT can allow just a few connections, or even no connections, to be established from the External Network to the NAT Network, as the user sees fit.

NAT Functionality

Of course NAT requires that some processor must translate the "private" network IP addresses to the "global" Internet IP address, and vice−versa. This is where routers using NAT come into the picture. This document explains how NAT was developed for Compatible Systems devices on three example networks, and details how the routers are configured using the Command Line interface to properly do Network Address Translation.

Note: The Command Line interface is currently the only way to configure the NAT functionality. CompatiView NAT functionality is in development, but not yet available.

A Compatible Systems router with NAT functionality enabled will do one of the following to IP packets sent through a NAT interface:

1. Translate an IP address and otherwise modify an IP packet if its address matches one of the NAT IP address ranges defined for the router.
2. Allow the router to accept and process the IP packet if that packet is addressed to the router itself (e.g., broadcast packets, a Telnet session to the router, or pinging the router).
3. Allow the IP packet to be routed without modifying it, if the IP address of the packet is within the NAT PassThru Range defined for the router.
4. Drop the packet if none of the conditions in 1, 2, or 3 are met.

Conditions 1 and 2 are presented in **Example One** below. Condition 3 is presented in **Example Two**. Condition 2 can be thought of as a default subset of Condition 3, where the destination is the router itself rather than some local LAN configured with a global IP address and connected to the router on an IP interface different from the one connecting the router to the Internet.

NAT EXAMPLE NETWORKS

Example One (Figure 1): The simpler of the two NAT Examples. The IP Interface Ethernet 0 on the NAT Router connects to the Internet. Such an IP interface is called the External NAT Port in this document. Everything behind the NAT Router, connected to the Internal Ethernet Hub and the NAT Router, via IP interface Ethernet 1, is part of the NAT Network. IP interfaces such as Ethernet 1 are called the Internal NAT Port in this document.

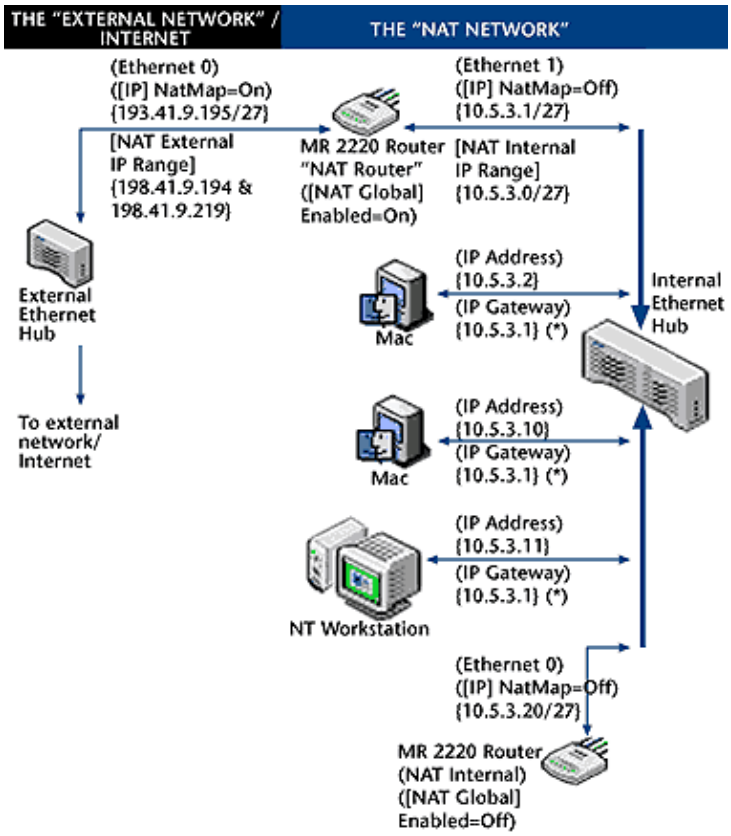
Example Two (Figure 2): WAN 0 (the External NAT Port) is the NAT IP interface connecting to the Internet; Ethernet 1 (the Internal NAT Port) connects to the NAT Network, but Ethernet 0 connects to an Ethernet hub which has "global" IP addresses. Ethernet 0, and its connected hub, are in effect part of the Internet. The Compatible Systems NAT software will allow the WAN 0 External NAT Port to pass IP packets to both the user's (Private) NAT Network and the LAN which has "global" IP addresses. The user can limit access to, or protect, the NAT Network while not effecting the performance of the portion of the network with "global" IP addresses.

Example Three: Very similar to **Example Two**, except that the External NAT Port, Internal NAT Port, and the port for the NAT PassThru Range are all located **on the same physical port**, by using sub−interfaces on this physical port.

EXAMPLE ONE

The **Example One** network, which was used in the development of the NAT software at Compatible Systems, is using a MicroRouter 2220R as the NAT Router. The NAT Router has IP port Ethernet 0 connected to the External Network and IP port Ethernet 1 connected to the NAT Network. Two Macintosh workstations, a PC running Windows NT and another MicroRouter 2220R are connected to the NAT Network Internal Ethernet hub. Other workstations and routers are connected to the External Ethernet hub, but, for clarity, only the connections to the NAT Router and the router connected to the Internet are shown here.

Figure 1



(*) NOTES: All of the machines in the NAT network must address their IP packets to the Internal Interface of the "NAT" MR 2220 Router (Ethernet 1).

Several important points about Compatible Systems NAT implementation are shown in **Figure 1**, and warrant special mention here:

1. The NAT functionality must be enabled in the router intended to do Network Address Translation. This is done by setting the Enabled variable (Enabled = On) in the [NAT Global] section. This will be described in more detail later in the NAT CONFIGURATION SECTION. In **Example One**, the NAT Router is the router between the NAT Network and the Internet.
2. The IP interface that communicates with the Internet must also be enabled for NAT. This is done by setting the NatMap variable (NatMap = On) on this interface in the [IP <Section ID>] section. This will also be described in more detail later in the NAT

CONFIGURATION SECTION. In **Example One** this is the Ethernet 0 IP interface.

3. The IP Interface which is communicating with the External Network or Internet must be the **only** interface which has NatMap = On. It is important that one, and only one, IP interface on a NAT Router have its NatMap variable set to On.

Point C is probably the most important, and least obvious, configuration requirement. In **Example One**, Ethernet 0 and Ethernet 1 both seem to be participating in Network Address Translation. The user could assume that NatMap could be set to On in both IP ports. THIS IS NOT THE CASE! Only Ethernet 0 should have NatMap = On. Compatible Systems NAT software will not function between two IP ports which both have NatMap = On.

Again, in Compatible Systems routers with the [NAT Global] variable Enabled=On, the single IP interface which has NatMap = On is called the External NAT Port. The IP interface connected to the "private" IP addresses is called the Internal NAT Port. In **Example One**, Ethernet 0 is the External NAT Port and Ethernet 1 is the Internal NAT Port.

NAT only translates the address of the workstations/routers in the NAT Network. It does not need to adjust the address of the location on the External Network. The MicroRouter 2220R NAT Router just makes the workstations/routers in the NAT Network **appear** to be at the Internet IP addresses of 198.41.9.194 or 198.41.9.219 and accessible through the IP interface of Ethernet 0 on this router. The sub−interface makes the Internet address assignment based on logic in the software. These translations are done using Translation Sessions (also called NAT Sessions) in the NAT software. One NAT Session is created for each IP Communication Session that is established through the NAT Router.

Since NAT can be viewed and is often used as a type of firewall, Point B makes sense. The previous paragraph also helps explain the reason for Point B. NAT must modify packets destined for, and coming from, the External Network/Internet. The NAT Router IP interface which most directly communicates with the Internet must be the one doing Network Address Translation (NatMap = On).

Except for one special condition, which will be explained shortly, IP sessions can only be established between the Internet and the NAT Network through the NAT Router by locations on the NAT Network (only from the inside to the outside).

Note: NAT functionality is available on Compatible Systems router IP interfaces with one important exception. A WAN interface can be used as the External NAT Port **only** if its IP address is assigned in the Router's configuration. NAT **cannot** function on WAN interfaces that have their IP address assigned by a dial−up, PPP negotiation.

AN EXAMPLE NAT SESSION (CONDITION 1)

The Mac at internal address 10.5.3.10 is going to ping the Internet location 128.138.240.11. The Mac sends its IP packets (ICMP Echo Requests) to its Gateway IP address of 10.5.3.1. This is the address of the Internal NAT Port on the NAT Router (Ethernet 1) which is connected to the NAT Network. At this point the NAT Router begins to create a NAT Session for this IP session. This NAT Session contains information about:

- the NAT Network location (Internal NAT) source IP address {10.5.3.10}
- the Internet location (Remote) IP destination address {128.138.240.11}
- the External, translated NAT (External NAT) IP source address it will use in translating the packet {198.41.9.219}
- and the Application Protocol being transmitted by the IP packets (ICMP).

On outbound packets, all Internal NAT source IP address entries {10.5.3.10} in the packet are changed to the External NAT IP address {198.41.9.219}.

On inbound packets, in response, all External NAT destination IP addresses {198.41.9.219} are changed to Internal NAT IP addresses {10.5.3.10}.

The NAT Session, which was created by the outbound IP packet from the NAT Network, is what allows this translation to take place.

NAT Sessions can be displayed in the Command Line interface with the command **show nat sessions**.

```
Nat_2220> show nat sessions
              Active Map                          Remote         Proto   Hashes
------------------------------------- -------------------- ------ ---------
10.5.3.10:0          ->198.41.9.219:0       128.138.240.11:0     ICMP   221/909
```

A NAT Session stores the three IP addresses as two pairs of IP addresses (or "hashes"): the hash of the "Remote" IP address and "External NAT" address (the "Mapped Hash"), and the hash of the "Remote" IP address and the "Internal NAT" address, and the Application Protocol of the IP session which established the NAT Session (in this case, ICMP) (See **Table 1**).

Table 1

```
(The External or MAPPED "Hash")
128.138.240.11:0  198.41.9.219:0
                     |
                     |
{Protocol = ICMP}-->+  <<=========================>>  The "NAT SESSION"
                     |
                     |
198.138.240.11:0  10.5.3.10:0
          (The Internal "Hash")
```

The details of the NAT functionality for the MicroRouter 2220R NAT Router of **Figure 1** and **Table 1** are shown in **Table 2**.

Table 2

External Network IP Addreses	NAT Router IP Addreses			NAT Network IP Addreses
	External Range(s)	Gateway Address	Internal Range	
'Global' IP Addreses	198.41.9.194 &198.41.9.219	10.5.3.1	10.5.3.0	10.5.3.2 to 10.5.3.30

Once again, note that the remote Internet IP address, be it a source or destination address, is never changed. The processes on the outside never really "know" the address(es) of the processes communicating with them through the NAT Router.

The External Range term shown in **Table 2** could be confusing. It **is not** the address or addresses to which the processes inside the NAT Network are communicating, as the name might imply. The External Range(s) is (are) the IP address(es) the NAT algorithm is using to allow outside processes to communicate with the IP addresses in the NAT Network through the External NAT Port. The internal processes only route their IP packets through the NAT Router Gateway address(es) on the Gateway's Internal NAT Port(s). They address their packets to the outside IP addresses, not the Gateway Address. This is important to note

because other descriptions of NAT on the Internet have not explicitly said this and initially caused confusion.

CONDITION 1: A NAT SESSION INITIATED FROM THE OUTSIDE

Let's make one change to the network of **Example One** − the NT workstation is now a Web server. Is this possible with Compatible Systems NAT? If possible, is it really useful? For security (and practicality) reasons, NAT Sessions are generated by IP packets traveling from the NAT Network to the Internet. How could an outside user ever reach the NT Web server on the NAT Network if the server did not first contact the user on the Internet (a highly unlikely situation)?

This is where another part of the Compatible Systems NAT software is useful. It is called the NAT Map Database. This database contains pairs of IP addresses (or IP address:TCP/UDP port combinations) which allow sites on the Internet to have access through the NAT Router to the NAT Network. The Internet sites can initialize NAT Sessions with sites on the NAT Network.

The NAT Map Database can be displayed in the Command Line interface with the command **show nat map**.

```
Nat_2220> show nat map

[ Nat Map Database ]
Total Number of Entries in NAT Map Database: 1
------------------------------------------------------
                 Internal                        External
LineNo. <IPaddress[/Mask or :Port]> -> <IPaddress[/Mask or :Port]>
   1    <10.5.3.11/32>              -> <198.41.9.194/32>
```

The user on the Internet could now access the IP address 198.41.9.194 and the NAT Router would allow access to the NT Station on the NAT Network at address 10.5.3.11. They can be viewed as "one−to−one translation pairs."

Of course, the user could access everything else in the Web server with this configuration. A more secure NAT Map Database entry would only allow the external user access to the NT station as a Web Server. This could be done by modifying the NAT Map Database entry to the following form:

```
10.5.3.11:80 -> 198.41.9.195:80
```

The NAT Map Database entry is always entered with the Internal IP address first, followed by a space, followed by a "−>" (a single equal sign "=" could be used instead), followed by a space, followed by the IP address all External/Internet users will access. See the EDIT CONFIG NAT MAPPING section for more details.

AN EXAMPLE NAT SESSION USING A NAT MAP DATABASE ENTRY

(CONDITION 1.A)

A site on the Internet at 128.138.240.11 attempts to establish an IP session with the Web Server at 10.5.3.11 on the NAT Network. The site at 128.138.240.11 has no information that the NAT Web server is at 10.5.3.11; rather the NAT Map Database entry of:

```
10.5.3.11:80 -> 198.41.9.195:80
```

allows the NAT Router to make the NAT Web server appear to be at 198.41.9.194. This NAT Map Database entry allows the NAT software to create a NAT Session when the site at 128.138.240.11 initiates an IP session to the NAT External Range IP address:port combination of 198.41.9.195:80. Remember that the NAT software cannot establish a NAT Session initiated by a source on the External Network/Internet unless such a "one−to−one" translation pair is defined in the NAT Map Database.

The NAT software will now translate packets from the Internet with the destination IP address:TCP port combination of 198.41.9.195:80 to the destination of 10.5.3.11:80. The NAT software will translate packets from the NAT Web server with a source of 10.5.3.11:80 to a source of 198.41.9.195:80 before routing them out of the External NAT Port.

PINGING THE NAT ROUTER (CONDITION 2)

This is a relatively simple situation. A source on the Internet sends an ICMP Echo Request Packet to IP address 198.41.9.195 (the IP address of Ethernet 0 on the NAT Router). The NAT Router does not do a Network Address Translation on the packet. The destination address is not in the NAT External Range of 198.41.9.194, 198.41.9.195 or 198.41.9.219. It is accepted by the NAT Router for processing. The NAT Router generates an ICMP Echo Reply packet and transmits it out Ethernet 0 to the source IP address from the ICMP Echo Request packet.

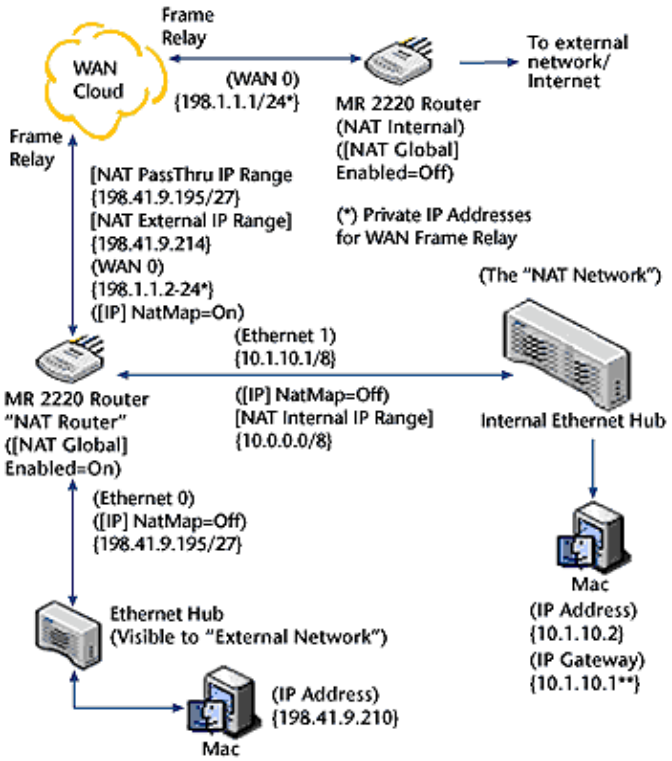
EXAMPLE TWO

This example demonstrates the functionality of the PassThru Range of Compatible Systems NAT software.

Example Two uses one Compatible Systems MicroRouter 2220R router to connect to the Internet through WAN 0 (the External NAT Port), to the NAT Network, with "private" IP addresses, through Ethernet 1 (the Internal NAT Port), and to part of the user's Network, which has "global" IP addresses, through Ethernet 0.

The part of the user's network connected to NAT Router Ethernet 0 is really part of the Internet. The External NAT Interface of WAN 0 connects to the WAN 0 of another router and to the Internet. This second router, even though it is shown in **Figure 2**, is not important to this example, except for the fact that it routes packets with addresses in the NAT PassThru Range to the WAN 0 External NAT Port of the NAT Router.

Figure 2



(*) NOTES: Private IP Addresses for the Frane Relay connection across the "WAN Cloud".

(**) NOTES: All of the machines in the NAT network must address their IP packets to the Internal Interface of the MR 2220 "NAT Router" (Ethernet 1).

Unlike **Example 1**, only part of the network behind this NAT Router is actually a NAT Network. Again, the part of the IP network connected to Ethernet 0 is accessible as part of the Internet. External sources can communicate with **almost** all of the IP addresses on Ethernet 0 without restriction. WAN 0 is the External NAT Port, Ethernet 1 is the Internal NAT Port and Ethernet 0 is not really involved with Network Address Translation; it just directly connects a portion of the user's network using "global" IP addresses to the Internet.

The NAT PassThru Range (198.41.9.195/27 in this case) allows the NAT Router to transmit IP packets between WAN 0 and Ethernet 0 as if the NAT Router is not even using NAT. However, NAT functionality does exist for the WAN 0 IP interface of the NAT Router.

PACKETS FROM THE NAT NETWORK THROUGH ETHERNET 1

(CONDITION 1, AGAIN)

The NAT Network packets, from the "private" IP address range of 10.0.0.0/8, are translated as they travel through the NAT Router and appear on the External Network to originate from the IP source address of 198.41.9.214. Packets from the External Network in response, with the destination IP address 198.41.9.214, will be translated to the proper "private" 10.0.0.0/8 network address by the NAT Router and transmitted through IP Interface Ethernet 1 to the NAT Network.

As has been previously stated, only sites on the NAT Network may create NAT Sessions for IP Address Translation unless one or more NAT Map Database one−to−one translation pairs exist in the [NAT Global] Configuration. None of these pairs exist in this example. All communication between the NAT Network and External Network must be initiated by the NAT Network. This example demonstrates two other important aspects of the Compatible

Systems NAT functionality:

1. The NAT External Range in the NAT Router does not have to be directly related to the IP address of the External NAT Port. However, the NAT External Range does have to be a "global" IP address and it must be "routable." The network must be able to deliver IP packets with addresses in the NAT External Range to the External NAT Port.
2. The designation of an IP address as part of the NAT External Range has a higher priority than the designation of that same IP address as part of the NAT PassThru Range in the Compatible Systems sub−interface. Even though the IP address of 198.41.9.214 is included as part of the NAT PassThru Range (198.41.9.195/27), its designation as part of the NAT External Range takes precedence. The IP address 198.41.9.214 will be part of the NAT External Range.

PINGING THE MACINTOSH AT 198.41.9.210 (CONDITION 3)

A site on the Internet sends an ICMP Echo Request packet to the Macintosh at IP address 198.41.9.210. The ICMP packet arrives at the NAT Router WAN 0 IP Interface, the External NAT Port. The IP destination address is within the NAT PassThru Range of 198.41.9.195/27, and **is not** within the NAT External Range of 198.41.9.214, so the NAT Router does not do any Network Address Translation to the packet. The ICMP packet is transmitted out IP Interface Ethernet 0 to the Macintosh.

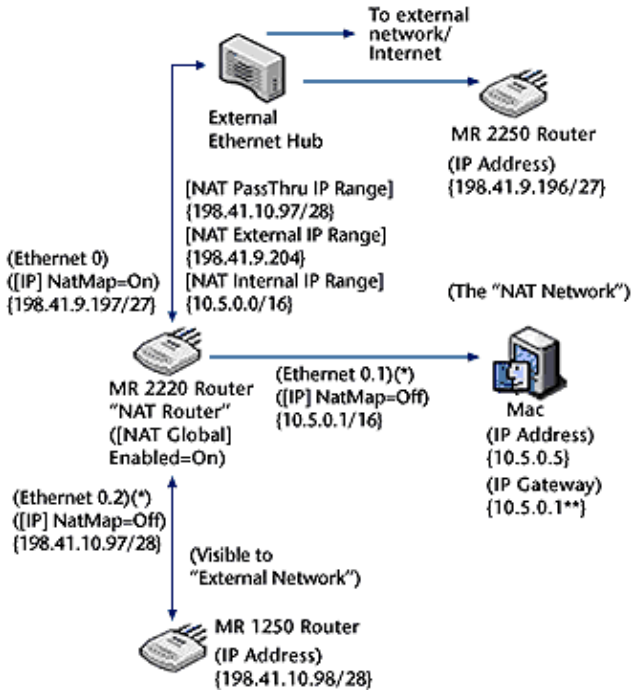
The Macintosh replies with an ICMP Echo Reply packet that enters the NAT Router from Ethernet 0. The NAT Router determines that the packet is destined for the External NAT Port with NatMap = On, but the source IP address is within the NAT PassThru Range, and not in the NAT External Range. The router does not translate the source IP address of the packet and simply transmits this ICMP Echo Reply packet out WAN 0 and to the source on the Internet which sent the ICMP Echo Request.

EXAMPLE THREE

This example demonstrates the functionality of the Compatible Systems NAT software to configure the External NAT Port and Internal NAT Port on the same physical port (Ethernet 0 in this example) using sub−interfaces.

Example Three uses one Compatible Systems MicroRouter 2220R Router to connect to the Internet through Ethernet 0 (the External NAT Port), to the NAT Network (with "private" IP addresses) through Ethernet 0.1 (the Internal NAT Port), and to part of the user's Network, which has "global" IP addresses, through Ethernet 0.2. The part of the user's network connected to NAT Router Ethernet 0.2 is really part of the Internet. The External NAT Interface of Ethernet 0 connects to the Internet via another device (not shown) connected to the same Ethernet hub as Ethernet 0.

Figure 3



(*) NOTES: IP sub−interface ports Ethernet 0.1 and 0.2 are shown as seperate connections in FIGURE 3 for clarity, but they really connect through the physical connection of Ethernet 0 and the "External Ethernet Hub" to the MR 1250i Router at IP address 198.41.10.98, the MR 2250R Router at IP address 198.41.9.196 and Macintosh at the NAT 'private' address of 10.5.0.5.

(**) NOTES: All of the machines in the NAT network must address their IP packets to the NAT Internal Interface of the MR 2220R "NAT Router" (Ethernet 0.1).

This example is very similar to **Example Two**, with an External NAT Port, Internal NAT Port, and NAT PassThru Range Port; but unlike **Example Two**, all of these ports exist on a **single** physical port of the MicroRouter 2220R NAT Router, through the use of sub−interfaces on the physical port Ethernet 0. The MicroRouter 2250R and MicroRouter 1250i are not involved with the NAT Network address translations in any way, but were included in the test network to prove that IP packets could be routed from the Internet to both devices. The MicroRouter 2250R is located on the network segment that includes the External NAT Port. The MicroRouter 1250i is accessed through the NAT PassThru Range of the MicroRouter 2220R NAT Router.

As for **Example Two**, the network segment attached to Ethernet 0.2 of the NAT Router and the MicroRouter 1250i are part of the Internet and have "global" IP addresses. The network segment attached to Ethernet 0.1 of the NAT Router and the Macintosh at IP address 10.5.0.5 are part of the NAT Network and have "private" IP addresses chosen by the user and can only communicate with the Internet if the MicroRouter 2220R NAT Router translates IP addresses being exchanged between the NAT Network and the Internet. The user has control over the access between the NAT Network and the Internet, through the configuration of the NAT variables in the MicroRouter 2220R.

IMPORTANT NOTE FOR USING NAT ON PORTS WITH SUB−INTERFACES ON THE SAME PHYSICAL PORT

The user **must** use Compatible Systems device software **version 4.4.02 OR LATER** to enable NAT on routers which have the Internal NAT Port and External NAT Port on the same physical port through the use of a sub−interface. The same is true if the user is configuring a sub−interface (e.g. WAN 0.1 or Ethernet 0.1) as the External NAT Port, even if the Internal NAT Port is on a different physical port of the router.

CONCLUDING EXPLANATION REMARKS

If these example explanations have not made the functionality of Network Address Translation a little clearer, please see one of the Web sites listed at the beginning of the document for more explanation.

If at least the basic ideas of Compatible Systems NAT implementation are understandable to you, please continue on to the next section which describes the Command Line commands used to configure the NAT software keywords in Compatible Systems routers and display the current status of the NAT software in the router.

CONSOLE COMMANDS FOR THE NAT SOFTWARE

SHOW NAT

The Network Address Translation software has a **show** command much the same as that of other features in Compatible Systems routers. The **show nat** command will produce the following display.

```
Nat_2220> show nat
Valid subcommands of nat are:
     Config                    NAT Configuration
     Map                       NAT Routing Map
     SEssions                  Active NAT Sessions
     STatistics                NAT Statistics
     Address_db                NAT IP Address Database
```

The five different options for the **show nat** command are almost self−explanatory but are described in more detail here.

- **show nat config** will show the current configuration of the NAT software in the router
- **show nat map** will display the one−to−one address translation pairs currently entered in the router, or display a message that no one−to−one address pairs are presently entered in the NAT Map Database
- **show nat sessions** will display the translation sessions currently active in the router's NAT software
- **show nat statistics** will display the total number of sessions the router has created since it was lasted booted, how many are currently active and the status of those sessions which are no longer active
- **show nat address db** will show all of the IP addresses being used by the router for Network Address Translation

The Command Line displays for each of these commands is shown and described in the following text.

SHOW NAT CONFIG

The following display is for the NAT Router of **Example Two**.

```
Nat_2220> show nat config
NAT functionality enabled (On/Off):                 On
NAT Response to external ICMPs (On/Off):            On
Communicate w/ Router through IP Ports (On/Off):    On
Configured Ports:                       Ether0
UDP timeout period (sec.):              300
TCP timeout period (sec.):              86400
TCP SYN timeout period (sec.):          180
```

```
TCP FIN timeout period (sec.):          180
Entered Internal ranges(s):             10.5.3.0/27

Entered External ranges(s):             198.41.9.219
                                        198.41.9.195
                                        198.41.9.194

Entered Pass Thru ranges(s):            198.41.9.{205-210}

[ NAT Map Database ]
Total Number of Entries in NAT Map Database: 2
------------------------------------------------------------
                 Internal                          External
LineNo.  <IPaddress[/Mask or :Port]> -> <IP address[/Mask or :Port]>
   1                   ->
   2                   ->
```

The line-by-line description of this display follows.

```
NAT functionality enabled (On/Off):     On
```

This variable must be On (the current default value is Off) to allow the router to do Network Address Translation on any of its IP ports.

Note: Another NAT variable in the IP port must also be turned On for that port to perform Network Address Translations. This will be described in more detail later.

```
NAT Response to external ICMPs (On/Off):     On
```

This variable must be On (the current default value) to allow any routers or workstations inside the NAT Network, behind the NAT Router, to respond to pings coming from outside the NAT Network. The router or workstation inside the NAT Network must have its address mapped to an address in the NAT External Range to allow the ICMP Echo Request packet through the NAT Router to the "private" IP address on the NAT Network.

```
Communicate w/ Router through IP Ports (On/Off):     On
```

This variable must be On (the current default value) to allow the router to communicate through the addresses of its IP ports. This is part of Condition 2 described earlier and includes Telnet sessions and pings to the NAT Router.

```
Configured Ports:     Ether0
```

This line lists the IP port which is currently doing Network Address Translation in the router.

Note: The NAT software is currently designed to allow only **one** IP port on a router to be doing Network Address Translation.

```
UDP timeout period (sec.):     300
```

The router will remove an active NAT Session for UDP (and all other non-TCP protocols) after 300 seconds (five minutes) if no IP sessions have used this NAT Session.

```
TCP timeout period (sec.):     86400
```

The router will remove an active NAT Session for TCP after 86400 seconds (24 hours) if no IP Network Address Translations have used this NAT Session.

```
TCP SYN timeout period (sec.):     180
```

The router will remove an active NAT Session for TCP after 180 seconds (three minutes) if a SYN TCP packet has not been answered.

```
TCP FIN timeout period (sec.):     180
```

The router will remove an active NAT Session for TCP after 180 seconds (three minutes) if a FIN TCP packet has not been answered.

```
Entered Internal range(s):     10.5.3.0/27
```

This is the Internal Range to/from which the Network Address Translation software will translate the IP address in packets destined for, or coming from, the Internal NAT Network through the Internal NAT Port. The subnet mask syntax for this variable is identical to that used for IP ports and filters in Compatible Systems routers. The "/27" is analogous to a subnet mask of 255.255.255.224. The first 27 of the 32 bits in the subnet mask are 1's. There can be multiple entries for the NAT Internal Range. These IP address ranges are local to the user's NAT Network and can be chosen by the user.

```
Entered External range(s):     198.41.9.219
                               198.41.9.195
                               198.41.9.194
```

This is the External Range to/from which the Network Address Translation software will translate the IP address in packets destined for, or coming from, the Internet through the External NAT Port. The subnet mask syntax for this variable is identical to that used for IP ports and filters in Compatible Systems routers. These three external ranges are actually individual IP addresses with subnet masks of 255.255.255.255. There can be multiple entries for the NAT External Range. These IP address ranges must be "global" Internet addresses. If a "global" IP address is included in both the NAT External Range and the NAT PassThru Range (explained next), the IP address will be treated as being part of the NAT External Range **only**.

```
Entered Pass Thru range(s):     198.41.9.{205-210}
```

This is the range of "global" IP addresses that **will not** be translated by NAT as they travel through the External NAT Port. This is only if the IP address in question is not within the NAT External Range (described above). If the IP destination address of packets coming into the External NAT Port, or IP source addresses of packets going out of the External NAT Port, fall within this IP address range, the packet will not undergo Network Address Translation. It will be routed like any IP packet in any IP router. As stated before, the designation of an IP address or IP address range as being part of the External NAT Range has precedence over the designation of those IP address(es) as being part of the NAT PassThru Range.

```
[ NAT Map Database ]
Total Number of Entries in NAT Map Database: 2
------------------------------------------------------------------
                Internal                          External
LineNo. <IPaddress[/Mask or :Port]> -> <IPaddress[/Mask or :Port]>
   1                  ->
   2                  ->
```

This section of the display shows the one-to-one address translation pairs entered in the NAT software. Each line of the display is read as the Internal Address (10.5.3.20, in line 2) which is translated to/from the External Address (198.41.9.194, in line 2). Packets addressed to 198.41.9.194 from the Internet will be accepted by the router, translated to the destination

address 10.5.3.20 and sent to the Internal NAT Network by the router.

Line 1 shows a different option for the one−to−one address translation pairs. It lists IP address:port combinations such that a site on the Internet could access a Web server on the workstation at the NAT Network address of 10.5.3.11.

SHOW NAT MAP

This display was described at the end of the previous section, but several other details will be presented here.

```
Nat_2220> show nat map
[ NAT Map Database ]
Total Number of Entries in NAT Map Database: 2
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
                Internal                        External
LineNo. <IPaddress[/Mask or :Port]> −> <IPaddress[/Mask or :Port]>
   1                  −>
   2                  −>
```

As noted previously, individual sockets (IP Address and Port combinations) can be entered and displayed as one−to−one pairs.

For example:

```
1    −>
```

is entered to allow a workstation at the Internal NAT Network address of 10.5.3.11 to be seen as a Web server on the Internet (the External Network) at the IP address of 198.41.9.194.

The one−to−one pairs can also map ranges of IP addresses such as:

```
X     −>
```

One important relationship between the NAT Map Database and the entered Internal and External Range(s) of NAT must be introduced here:

> The Internal half of the one−to−one pair **must** be within the NAT Internal Range of the configuration, and the External half of the one−to−one pair **must** be within the NAT External Range of the configuration.

The NAT software will not use a one−to−one pair in the NAT Map Database which fails to meet the above criteria.

SHOW NAT SESSIONS

This command will display all active NAT Sessions that the NAT software is presently using to modify IP packets as they travel between the NAT Network and the External Network/Internet.

```
Nat_2220> show nat sessions
              Active Map                          Remote         Proto   Hashes
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
                                 Time Since: Created              Last Activity
                                             −−−−−−−−−−−−−−−−−    −−−−−−−−−−−−−−−−
10.5.3.20:0          −>198.41.9.194:0        198.41.9.200:0        ICMP   221/907
                                             124.33                114.33
```

```
10.5.3.20:0          ->198.41.9.194:0       198.41.9.215:0       ICMP   236/922
                                            105.00               104.00
10.5.3.10:29841      ->198.41.9.219:29841   198.41.9.30:53       UDP    255/976
                                            33.93                33.50
10.5.3.10:1899       ->198.41.9.219:1899    198.41.9.12:80       TCP    983/680
                                            25.67                0.16
10.5.3.10:1900       ->198.41.9.219:1900    198.41.9.12:80       TCP    984/681
                                            30.24                15.83
```

The Active Map is the IP Address:Port (if applicable) Internal to External address translation and is read in the same format as the display for the NAT Map Database. The Remote is the location on the External Network/Internet communicating with the workstation or router in the Internal NAT Network. The Proto is the protocol the session is translating. Current values for this column are ICMP, UDP, TCP, GRE, OSPF, EGP, ESP, AH, BLAST, or the actual number of the other IP protocols. The hashes are used by the software to store and locate the translation sessions in the NAT software's internal database. The Time Since: Created, and Last Activity display the time, in seconds, since the session was created and the last time it was used to translate an IP packet, respectively.

SHOW NAT STATISTICS

The **show nat statistics** command displays the total number of NAT Sessions created since the router was last booted with the NAT functionality enabled, and the current status of the NAT Sessions.

```
Nat_2220> show nat statistics
Total Sessions:                    38
  Filtered:                         0

 Currently Active:                  0

 Properly Removed:                 33

 Sessions Timed Out:                5
  SYN Timeouts:                     0
  FIN Timeouts:                     0
  Inactivity:                       5


 Sessions Reset:                    2
  Invalid Cache:                    0
  No Resources:                     0
  Stale ACK:                        0
```

Total Sessions is the total number of NAT Sessions created to translate IP packets since the router was last booted.

Filtered is not yet defined.

Currently Active is the number of packets presently being used by the router to translate packets. This should be displayed in response to the command **show nat sessions** (described earlier) if these sessions have not been ended/removed from the NAT hash database by the software in the meantime.

Properly Removed is the number of sessions removed from the NAT Session database as a result of FIN and ACK packets being exchanged between the workstation/router on the NAT Network and the workstation/router on the Internet. The IP session is terminated and the NAT Session doing the address translation is likewise removed from the NAT hash database.

Sessions Timed Out is the number of NAT Sessions removed from the NAT hash database as a result of a time limit being exceeded. This can occur in one of three ways:

1. a SYN packet in a session does not receive a response within the time limit defined by the NAT variable "TCP SYN timeout period" (described earlier); these are tallied in SYN Timeouts
2. a FIN packet in a session does not receive a response within the time limit defined by the NAT variable "TCP FIN timeout period" (described earlier); these are tallied in FIN Timeouts
3. the session has not been used for any IP address translations in the time limit defined by either "UDP timeout period" or "TCP timeout period" (both described earlier); these are tallied in Inactivity

Currently, all non−TCP NAT Sessions use the NAT variable UDP timeout period for their inactivity timeout limits.

The sum of the values for Currently Active, Properly Removed, and Sessions Timed Out **should** be equal to the value for Total Sessions.

Sessions Reset tallies the NAT Sessions for which a RST packet was sent.

The Invalid Cache, No Resources, and Stale ACK values are not yet being used.

SHOW NAT ADDRESS_DB

The command **show nat address_db** shows the IP address database the NAT software is using to do IP address translations. This display contains a lot of information that needs some explanation.

```
Nat_2220> show nat address_db
Network Address Translation Address Database
Address Tree Level  IP Address          IP Mask    Flags
------------------- ------------------- ---------- ----------
+                   10.5.3.0            0xfffffffe0 0x00000001
++                  10.5.3.1            0xffffffff 0x00010000
++                  10.5.3.11           0xffffffff 0x00000111
++                  10.5.3.20           0xffffffff 0x00000011
+                   198.41.9.192        0xfffffffe0 0x00010000
++                  198.41.9.194        0xffffffff 0x00000012
++                  198.41.9.195        0xffffffff 0x00001112
++                  198.41.9.205        0xffffffff 0x00000004
++                  198.41.9.206        0xffffffff 0x00000004
++                  198.41.9.207        0xffffffff 0x00000004
++                  198.41.9.208        0xffffffff 0x00000004
++                  198.41.9.209        0xffffffff 0x00000004
++                  198.41.9.210        0xffffffff 0x00000004
++                  198.41.9.219        0xffffffff 0x00000002
Flag Legend:  INTERNAL: 0x0001, MAPPED: 0x0002, PassThru: 0x0004
              PORT in MAP_DB: 0x0010, 1 to 1: 0x0100, ROUTER IP PORT: 0x1000
              PLACEHOLDER: 0x00010000
```

The above IP address database could better be viewed in a "tree form" such as:

```
     Highest Level (+)               Next Highest Level (++)
     -----------------               -----------------

     10.5.3.0 (#) ---------+--------- 10.5.3.1($)
     (255.255.255.224)     |
                           +--------- 10.5.3.11(#)(%)()
```

```
                          |
                          +--------- 10.5.3.20(#)(%)


     198.41.9.192 ---------+--------- 198.41.9.194(@)(%)
     (255.255.255.224)     |
                          +--------- 198.41.9.195($)(@)(%)()

                          |
                          +--------- 198.41.9.205(*)
                          |
                          +--------- 198.41.9.206(*)
                          |
                          +--------- 198.41.9.207(*)
                          |
                          +--------- 198.41.9.208(*)
                          |
                          +--------- 198.41.9.209(*)
                          |
                          +--------- 198.41.9.210(*)
                          |
                          +--------- 198.41.9.219(@)

                          (all have masks of 255.255.255.255)

(#)   Part of the "NAT INTERNAL RANGE"
($)   One of the "NAT Router" IP Port addresses
(%)   Part of a 1 to 1 translation pair in "NAT Map Database"
()  Ports are defined for this part of the 1 to 1 translation pair
(@)   Part of the "NAT EXTERNAL RANGE"
(*)   Part of the "NAT PASSTHRU RANGE"
```

The IP Mask column is the hexadecimal representation of the mask associated with each address.

The Flags column is the summation of all flags that apply to each IP address in the NAT Address Database. The flags are defined briefly in the Flag Legend at the end of the display and each and is important for NAT functionality. Detailed descriptions of each flag will not be presented here.

CONFIGURATION SECTION

The next two sections show an example of configuring a Compatible Systems MicroRouter 2220R router to perform Network Address Translation. They also give more detailed description of the NAT functionality in Compatible Systems routers.

The agreement of the [NAT Global] configuration and [IP <Section ID>] configuration on the router ports is the most important aspect of NAT functionality in Compatible Systems routers. The [NAT Global] configuration will be described first, followed by the required parts of the [IP <Section ID>] configuration for proper NAT functionality.

[NAT Global]

The [NAT Global] variables are configured in the same way as other global sections in the router. The displayed messages are much the same as for all the other sections.

```
Nat_2220> configure nat global
Enter Password: (password entered)

Configure parameters in this section by entering:
```

```
   <Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"

[ NAT Global ]# ?
Valid keywords for the 'NAT Global' section:
        UDPTimeout              UDP Timeout for NAT in seconds
                                (note: 0 {zero} disables UDPTimeout)
        TCPTimeout              TCP Timeout for NAT in seconds
                                (note: 0 {zero} disables TCPTimeout)
        TCPSynTimeout           TCP SYN Timeout for NAT in seconds
        TCPFinTimeout           TCP FIN Timeout for NAT in seconds
        InternalRange           Strings for Internal IP addresses,
                                (parsed like filters)
        ExternalRange           Strings for External IP addresses,
                                (parsed like filters)
        PassThruRange           Strings for not NATTED IP addresses,
                                (parsed like filters)
        RespondICMP             NAT interface reponses to ICMP packets
        RouterAddr              Allow communication with a NAT router
                                through router IP ports
        Enabled                 Overall NAT capability in Router

Other useful commands:
     delete <keyword>        Delete a keyword in this section
     list                    Display the contents of current section
     <keyword> = ?           Display more information about a keyword
     help                    Information about other commands
```

All of these keywords have been introduced in the NAT "Show" Commands section and extra detail will be presented here.

```
     UDPTimeout     UDP Timeout for NAT in seconds
                    (note: 0 {zero} disables UDPTimeout)
```

The default value for removing a non−TCP NAT Session due to inactivity is 300 seconds (five minutes). It has a range from 0 to 3600 seconds (one hour). A value of zero will cause non−TCP NAT Sessions to never be removed due to inactivity. Use this option with caution because it is possible for the router memory to eventually be occupied by the NAT translation session database.

```
     TCPTimeout     TCP Timeout for NAT in seconds
                    (note: 0 {zero} disables TCPTimeout)
```

The default value for removing TCP sessions due to inactivity is 86400 seconds (24 hours). It has a range from 0 to 172800 seconds (48 hours). As for the UDPTimeout, a value of zero will cause TCP NAT Sessions to never be removed due to inactivity. Also use this option with caution because it is possible for the router memory to eventually be occupied by the NAT translation session database.

```
TCPSynTimeout     TCP SYN Timeout for NAT in seconds
     TCPFinTimeout     TCP FIN Timeout for NAT in seconds
```

The default value for these variables is 180 seconds (three minutes). They have a range of 20 to 300 seconds. They cannot be disabled.

```
InternalRange     Strings for Internal IP addresses,
                       (parsed like filters)
```

This is one of the two most important variables in the [NAT Global] section. This is the range of IP addresses that will be translated into the range of IP addresses set by the ExternalRange

(defined next). The NAT Router and the LANs and or WANs to which it is connected must be configured so that IP packets with addresses in the InternalRange enter the NAT Router through the Internal NAT Port.

This variable is parsed, and can be entered, using the same syntaxes used for the IP addresses in the IP filters with one important addition. An inclusive range of addresses can be defined using a dash notation (V.W.X.{Y−Z}). This was previously shown in the NAT PassThru Range part of the **show command** section. For example, an Internal Range could be entered as 10.5.3.{1−30}. This would be parsed as the IP addresses 10.5.3.1, 10.5.3.2, ... 10.5.3.29, and 10.5.3.30 (and every IP address in between, but omitted from listing here). Each of these parsed addresses would have a mask of /32 or 255.255.255.255.

This is a multiple variable and can have several different values/ranges entered into it.

```
ExternalRange     Strings for External IP addresses,
                       (parsed like filters)
```

This is the most important variable in the [NAT Global] section. Again, the NAT Router and the LANs and or WANs to which is connected must be configured such that IP packets with addresses in the ExternalRange enter the NAT Router through the External NAT Port.

This variable is parsed like the InternalRange (like IP filters and including the dash notation) and is a multiple variable which can have several different values/ranges entered into it.

```
PassThruRange     Strings for not NATTED IP addresses,
                       (parsed like filters)
```

This is not always used in a NAT Router, unless the user is putting both a NAT Network and a LAN with "global" IP addresses behind the NAT Router and its External NAT Port (see **Example Two** presented earlier). This variable allows IP packets traveling through the NAT External Port to be routed without having their IP addresses translated.

This variable is also parsed like the InternalRange and ExternalRange (like IP filters and including the dash notation) and is a multiple variable that can have several different values/ranges entered into it.

If an IP address or range of addresses is included in both the ExternalRange (NAT External Range) and PassThruRange (NAT PassThru Range), NAT will treat the IP address(es) as being members of the ExternalRange (NAT External Range).

```
     RespondICMP     NAT interface responses to ICMP packets
```

This allows external workstations/routers to ping workstations/routers in the NAT Network if a one−to−one translation pair in the NAT Map Database will allow such a translation (again, these pairs have been briefly described before, and will be detailed in EDIT CONFIG NAT MAP). This keyword is either On or Off. The default value is On. The workstation/router on the Internal NAT Network will not be allowed to respond to a ping if RespondICMP is Off.

```
RouterAddr     Allow communication with a NAT Router
                    through router IP ports
```

This allows the router to accept IP packets destined for the IP addresses of the NAT Router's ports, and to transmit IP packets sourced from the IP addresses of the NAT Router's ports. In short, it allows the user to ping or establish a Telnet session with the NAT Router if this variable is set to On (the current default value). If this variable is set to Off, the user will only

be able to communicate with/configure the NAT Router via the Command Line interface.

```
Enabled      Overall NAT capability in Router
```

After the InternalRange and ExternalRange, Enabled is probably the most important keyword in this section. It allows the router to perform Network Address Translations between the internal and External Networks. The default value is Off. The router will not "NAT" if Enabled is Off.

[NAT Mapping]

The one−to−one translation pairs of the NAT Map Database are entered with the **edit config** rather than the **configure** command. These pairs allow the user to provide access from the Internet/External Network to selected parts of the NAT Internal Network, such as a Web server, as was previously shown in the NAT "SHOW" COMMANDS section.

```
Nat_2220> edit config nat mapping
Enter Password: <Entered password>
Editing "[ NAT Mapping ]"...

  1: [ NAT Mapping ]
  2: 10.5.3.20 −> 198.41.9.194
End of buffer
Edit [ NAT Mapping ]> ?
Available Editor Commands:
        Append     Append lines into the buffer
        Delete     Delete a line from the buffer
        Print      Print a range of lines
        List       Print a range of lines
                   (Non printing characters printed unambiguously)
        Help       Print this message
        Quit       Leave the editor (ignoring changes)
        Exit       Leave the editor (saving changes)
Edit [ NAT Mapping ]> append
Enter lines at the prompt.  To terminate input, enter
a . on a line all by itself.

Append>  10.5.3.11:80 −> 198.41.9.195:80
Append>  .
Edit [ NAT Mapping ]> exit
Saving section...
Checking syntax...
Section checked successfully.
*Nat_2220# save
Save configuration to flash and restart device? y

(Router will restart)
```

The NAT Map Database one−to−one translation pair is always entered with the internal IP address first, followed by a space, followed by a "−>" (a single equals sign "=" could be used instead), followed by a space, followed by the IP address all external/Internet users will access.

The router will check the syntax of the entered one−to−one pair for correctness. The IP addresses are parsed in the same way as IP addresses are parsed in the **add ip route** command, described in the **ip route (add)** section of the Text−Based Configuration and Command Line Reference Guide.

After rebooting, the NAT Map Database would look like...

```
Nat_2220> sh nat map

[ NAT Map Database ]
Total Number of Entries in NAT Map Database: 2
------------------------------------------------------------------
                Internal                        External
LineNo. <IPaddress[/Mask or :Port]> -> <IPaddress[/Mask or :Port]>
   1                  ->
   2                  ->
```

Important points about the one−to−one translation pairs in the NAT Map Database:

1. The Internal IP Address must be entered first, followed by "->" or " = ", followed by the External IP Address.
2. The Internal IP Address **must** be within the range of IP addresses defined by the [NAT Global] keyword InternalRange, and the External IP Address **must** be within the range of IP addresses defined by the [NAT Global] keyword ExternalRange.
3. The one−to−one pairs must either be both IP address:port combinations, or IP address ranges. An IP address:port combination **cannot** be paired with an IP address range (even if that range is a single IP address).
4. IF ONLY A SINGLE EXTERNAL IP ADDRESS IS AVALIABLE FOR THE NAT ROUTER, DO NOT MAP THAT IP ADDRESS TO AN INTERNAL IP ADDRESS! YOU WILL NOT BE ABLE TO CONTACT THE ROUTER THROUGH THE EXTERNAL NAT PORT TO COMMUNICATE WITH IT! Mapping single **ports** of the single external IP address to internal IP address:port combinations is acceptable, such as creating access to a Web server in the NAT Network (see **Example One**). Mapping the entire single external IP address (the router's IP Address) to an internal NAT address will prevent you from communicating with the router when NAT functionality is enabled.

Note: The [NAT Global] variable RouterAddr must also be set to On (the current default value) to allow the user to communicate with the NAT Router via IP over any of its IP ports.

[IP < Section ID >] PORT CONFIGURATION FOR NAT FOR EXAMPLE ONE

The IP ports on a Compatible Systems router performing Network Address Translation must be configured to be "in agreement" with the configuration of the [NAT Global] keywords or the router will not do Network Address Translation between the NAT Network and the External Network/Internet.

The configuration of the **Example One** Compatible Systems MicroRouter 2220R Router is shown below. The slightly more complex configuration of the NAT Router in **Example Three** is shown at the end of this section.

```
Nat_2220> show ip config

                              Addresses

Port            IP Addr       Subnet           Broadcast      Flags

Ethernet 0      198.41.9.195  255.255.255.224  198.41.9.223   <OSPF:off><RIP:out, in, V2>

                                                              <NAT>

Ethernet 1      10.5.3.1      255.255.255.224  10.5.3.31      <OSPF:off><RIP:out, in, V2>


Bridge          ** Disabled **
Wan 0           ** Disabled **
Wan 1           ** Disabled **
```

Ethernet 0 is the External NAT Port, Ethernet 1 is the Internal NAT Port. The IP protocol on the Bridge, Wan 0, and Wan 1 has been disabled in this example.

Note: Again, the NAT software is currently designed and has only been tested with **one** External IP Port on a router. In the latest releases of Compatible Systems device software (versions 4.3 and later), the display in response to the **show ip config** will display which IP interface has the variable NatMap enabled (NatMap = On).

The configuration setup of each IP Ethernet Port is shown below with the corresponding keywords from the [NAT Global] section. The "agreement" between the keywords of these sections is also shown.

EXTERNAL NAT PORT, EXAMPLE 1

The configuration of the External NAT Port and its relation to the [NAT Global] section is shown first.

```
Nat_2220> config ip ethernet 0
Enter Password:

Configure parameters in this section by entering:

   <Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"

[ IP Ethernet 0 ] # list
[ IP Ethernet 0 ]
Mode                    = Routed
RIPVersion              = V2
NatMap                  = On
SubnetMask              = 255.255.255.224
IPAddress               = 198.41.9.195
```

The most important keyword here is NatMap. If this keyword is **not** set to On, the IP Port will not perform Network Address Translation.

Note: The NatMap keyword needs to be turned On **only** on the External NAT Port. NatMap **should not** be set to On for the Internal Nat Port.

The other two IP port keywords that are critical for proper NAT performance are IPAddress and SubnetMask. The user must have the External NAT Port, and the network to which it is connected, configured such that IP packets with addresses within the NAT External Range enter the router through the NAT External Port.

In [NAT Global]:

```
     Entered External range(s):       198.41.9.219
                                      198.41.9.195
                                      198.41.9.194
```

and in [IP Ethernet 0]:

```
     SubnetMask              = 255.255.255.224
     IPAddress               = 198.41.9.195
```

The IP port must also have its Mode set to Routed.

INTERNAL NAT PORT, EXAMPLE 1

The configuration of the Internal NAT Port and its relation to the [NAT Global] section is shown next.

```
Nat_2220> config ip ethernet 1
Enter Password:

Configure parameters in this section by entering:

   <Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"

[ IP Ethernet 1 ] # list
[ IP Ethernet 1 ]
RIPVersion               = V2
Mode                     = Routed
SubnetMask               = 255.255.255.224
IPAddress                = 10.5.3.1
```

The NatMap is **not** set to On for this Internal NAT Port. It is still set to its default value of Off and not listed in the configuration.

```
[ IP Ethernet 1 ] # NatMap = ?
The keyword 'NatMap' expects Boolean values:
     Default:       Off
     Valid Values:  True/False, On/Off, 1/0, or Yes/No.
     Help String:   Enable Network Address Translation
```

Again, the user must have the Internal NAT Port, and the Network to which it is connected, configured such that IP packets with addresses within the NAT Internal Range enter the router through the NAT Internal Port.

In [NAT Global]:

```
     Entered Internal range(s): 10.5.3.0/27
```

and in [IP Ethernet 1]:

```
     SubnetMask  =  255.255.255.224
     IPAddress   =  10.5.3.1
```

Note: All workstations on the LAN directly connected to the Internal NAT Port must have this IP port's address (10.5.3.1, in this example) set as their Gateway route in their IP applications.

[IP < Section ID >] PORT CONFIGURATION FOR NAT FOR EXAMPLE THREE

This is the configuration of the NAT Router in the more complex **Example Three** that has NAT configured on a physical port that has sub−interfaces. Again see the IMPORTANT NOTE concerning the version of Compatible Systems router software required to use NAT on physical ports which have sub−interfaces configured. The [NAT Global] configuration and the [IP <Section ID>] configuration are shown below to demonstrate the "agreement" between these two sections of the device configuration.

Here is the [NAT Global] configuration section.

```
       NAT_2220R1> show nat config
```

```
NAT functionality enabled (On/Off):               On
NAT Response to external ICMPs (On/Off):          On
Communicate w/ Router through IP Ports (On/Off):  On
Configured Ports:                Ether0
UDP timeout period (sec.):       300
TCP timeout period (sec.):       86400
TCP SYN timeout period (sec.):   180
TCP FIN timeout period (sec.):   180
Entered Internal range(s):       10.5.0.0/24

Entered External range(s):       198.41.9.204

Entered Pass Thru range(s):      198.41.10.98/28

[ NAT Map Database ]
<no entries in NAT Map Database>
```

Here is the configuration of the IP ports.

```
NAT_2220R1> show ip config
                                Addresses
Port            IP Addr         Subnet             Broadcast      Flags
Ethernet 0      198.41.9.197    255.255.255.224    198.41.9.223   <OSPF:off><RIP:out,

                                                                  <NAT>

Ethernet 0.1    10.5.0.1        255.255.0.0        10.5.255.255   <OSPF:off><RIP:out,i


Ethernet 0.2    198.41.10.97    255.255.255.240    198.41.10.111  <OSPF:off><RIP:out,i

Ethernet 1     ** Disabled **
Bridge         ** Disabled **
Wan 0          ** Disabled **
Wan 0.1        ** Disabled **
Wan 1          ** Disabled **
```

Ethernet 0 is the External NAT Port, Ethernet 0.1 is the port to the NAT PassThru Range (which is accessible from the rest of the Internet) and Ethernet 0.2 is the Internal NAT Port. The IP protocol on the Bridge, Wan 0, and Wan 1 have been disabled in this example.

Note: Again, the NAT software is currently designed and has only been tested with **one** External IP Port on a Router. In the latest releases of Compatible Systems device software (versions 4.3 and later), the display in response to the **show ip config** will display which IP interface has the variable NatMap enabled (NatMap = On). This can be seen in the above display for Ethernet 0.

The configuration set up of each IP Ethernet Port is shown below with the corresponding keywords from the [NAT Global] section. The "agreement" between the keywords of these sections is also shown.

EXTERNAL NAT PORT, EXAMPLE 3

The configuration of the External NAT Port and its relation to the [NAT Global] section is shown first.

```
NAT_2220R1> config ip ethernet 0
Enter Password: (enter password)

Configure parameters in this section by entering:
```

```
<Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"
[ IP Ethernet 0 ] # list
[ IP Ethernet 0 ]
Mode              = Routed
RIPVersion        = V2
SubnetMask        = 255.255.255.224
IPAddress         = 198.41.9.197
NatMap            = On
```

The most important keyword here is NatMap. If this keyword is **not** set to On, the IP Port will not perform Network Address Translation.

Note: The NatMap keyword needs to be turned On **only** on the External NAT Port. NatMap **should not** be set to On in the Internal Nat Port.

The other two IP port keywords that are critical for proper NAT performance are IPAddress and SubnetMask. The user must have the External NAT Port, and the network to which it is connected, configured so that IP packets with addresses within the NAT External Range enter the router through the NAT External Port.

In [NAT Global]:

```
Entered External range: 198.41.9.204
```

and in [IP Ethernet 0]:

```
SubnetMask   = 255.255.255.224
IPAddress    = 198.41.9.197
```

The IP port must also have its Mode set to Routed.

INTERNAL NAT PORT, EXAMPLE 3

The configuration of the internal NAT port and its relation to the [NAT Global] section is shown next.

```
[ IP Ethernet 0 ] # config ip ethernet 0.1

Configure parameters in this section by entering:

<Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"
[ IP Ethernet 0.1 ] # list
[ IP Ethernet 0.1 ]
SubnetMask          = 255.255.0.0
IPAddress           = 10.5.0.1
NatMap              = Off
```

Again, the user must have the Internal NAT Port, and the network to which it is connected, configured such that IP packets with addresses within the NAT Internal Range enter the router through the NAT Internal Port.

In [NAT Global]:

```
Entered Internal range(s): 10.5.0.0/16
```

and in [IP Ethernet 0.1]:

```
SubnetMask  = 255.255.0.0
IPAddress   = 10.5.0.1
```

Notes: All workstations on the LAN directly connected to the Internal NAT Port must have this IP Port's address (10.5.0.1, in this example) set as their Gateway route in their IP applications.

NAT PASSTHRU RANGE, EXAMPLE 3

Finally, configuration of the other Ethernet IP sub−interface port and its relation to the [NAT Global] section are shown.

```
[ IP Ethernet 0.1 ] # config ip ethernet 0.2

Configure parameters in this section by entering:

<Keyword> = <Value>

To find a list of valid keywords and additional help enter "?"

[ IP Ethernet 0.2 ] #list
[ IP Ethernet 0.2 ]
IPAddress           = 198.41.10.97
SubnetMask          = 255.255.255.240
NatMap              = Off
```

As for the External and Internal NAT Ports, the router must be configured, or have the ability, to route the IP traffic addressed to and from the NAT PassThru Range. Also, the NatMap variable for this IP sub−interface is set to Off (the default value).

In [NAT Global]

```
Entered Pass Thru range(s): 198.41.10.98/28
```

and in [IP Ethernet 0.2]

```
IPAddress = 198.41.10.97
SubnetMask = 255.255.255.240
```

FINAL NOTES

The example Compatible Systems router is now ready to perform Network Address Translation.

Currently Supported IP Applications

1. All IP applications which **only** contain the IP source and IP destination addresses in the IP Packet Header (Telnet, HTTP, etc.)
2. File Transfer Protocol
3. NetBios for NT Workstations
4. CUSeeMe
5. Real Audio

Updated: Aug 19, 2004 Document ID: 17621